Privacy and Security Concerns in Generative AI: A Comprehensive Survey

Year: 2024 | *Citations: 120* | *Authors: Abenezer Golda, K. Mekonen, Amit Pandey*

Abstract

Generative Artificial Intelligence (GAI) has sparked a transformative wave across various domains, including machine learning, healthcare, business, and entertainment, owing to its remarkable ability to generate lifelike data. This comprehensive survey offers a meticulous examination of the privacy and security challenges inherent to GAI. It provides five pivotal perspectives essential for a comprehensive understanding of these intricacies. The paper encompasses discussions on GAI architectures, diverse generative model types, practical applications, and recent advancements within the field. In addition, it highlights current security strategies and proposes sustainable solutions, emphasizing user, developer, institutional, and policymaker involvement.